CLAIMS

We claim:

1. A method for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising the steps of:

determining whether a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement which will allow the particular sender to become a registered sender of email to the particular receiver;

weeding out at a gateway of the communication system all email directed to a particular receiver that originates from senders that are determined not to be registered senders to the particular receiver; and

passing to the particular receiver all email directed to the particular receiver and that originates from senders determined to be registered senders of email to the particular receiver.

2. The method of claim 1, wherein said determining step comprises the steps of:

setting up by the particular sender a cookie which indicates to the particular receiver whether the particular sender has satisfied the requirement to allow the particular sender to become a registered sender to the particular receiver;

setting up an address related to an address associated with the particular receiver which will inform the particular sender that the particular receiver desires that the particular sender be able to send email to the particular receiver; and

setting up by the particular receiver a key which is forwarded to the particular sender by the particular receiver to inform the particular sender that the particular sender is authorized to send email to the particular receiver and is now a registered sender and for use by the particular sender whenever the particular sender wishes to send email to the particular receiver.

3. The method recited in claim 2, wherein said step of setting up the address comprises generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

4. The method recited in claim 2, wherein said step of setting up an encrypted address comprises sending email from the particular receiver to the particular sender using public key encryption.

5. The method recited in claim 2, wherein said determining step further comprises sending to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

6. The method recited in claim 5, further comprising the step of storing the encrypted key by the particular sender in a table of encrypted keys for use by the particular sender whenever the particular sender desires to send email to the particular receiver.

7. The method recited in claim 1, wherein said weeding out step comprises:

examining a message authentication code (MAC) by the particular receiver and determining whether the examined MAC is a valid MAC; and

rejecting the email sent by the particular sender if the MAC is determined not to be a valid MAC.

8. The method of claim 7, wherein said step of MAC determining comprises comparing the MAC against a value determined in said sender determining step and, if the value and the determined MAC are the same, accepting by the particular receiver the email from the sender.

9. The method recited in claim 7, wherein said MAC determining step comprises comparing the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

10. A server method for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising:

a determining module for determining whether a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered

sender by satisfying a requirement which will allow the particular sender to become a registered sender of email to the particular receiver;

a weeding out module for weeding out at a gateway of the communication system all email directed to a particular receiver that originates from senders that are determined not to be registered senders to the particular receiver; and

a passing module for passing to the particular receiver all email directed to the particular receiver and that originates from senders determined to be registered senders of email to the particular receiver.

11. The server recited in claim 10, wherein said determining module further comprises a generator for generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

12. The server recited in claim 11, wherein said determining module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption.

13. The server recited in claim 13, wherein said determining module sends to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

14. The server recited in claim 13, wherein said weeding out module examines a message authentication code (MAC) by the particular receiver and determines whether the examined MAC is a valid MAC, and rejects the email sent by the particular sender if the MAC is determined not to be a valid MAC.

15. The method of claim 14, wherein said weeding out module compares the MAC against a value, and if the value and the determined MAC are the same, accepts by the particular receiver the email from the sender.

16. The method recited in claim 15, wherein the weeding out module compares the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.